# 准备：

1 十六进制编辑器 [推荐HxD 已附件]

2 要分析的ips [附件了压缩包 内含两个ips 用于练手]

适用于一些非大型ips，如全屏攻击，道具不减，无限血量等等，若是大型ips，

还是直接加载吧，我写的教程只提供思路，要用来做什么取决于自己

分析有两种情况，一种是未加密的，一种是加密的，我会把这两种情况都举栗

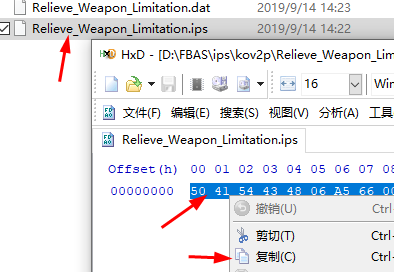
简单说，未加密的ips分析后地址对应的字节是和游戏里内存浏览区域显示一样的，

加密的虽然能分析出地址，但对应的字节却是加密的，

并且分析出的地址无法直接在ROM里定位到正确字节，

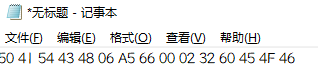
必须在游戏里用调试器浏览对应地址的内存区域才能获取到解密的字节，以制作作弊码

先分析未加密的，拿我之前制作的群雄205-解除武器限制ips举栗，



将ips文件拖入HxD，Ctrl+A全选字节，在其上右键选择复制或Ctrl+C，

打开记事本粘贴，

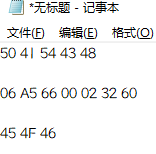


50 41 54 43 48 这几个字节是ips的文件头，

删除48后的空格，并回车两次分开内容和文件头

而45 4F 46是ips的文件尾，

同样删除45之前的空格，并回车两次分开内容和文件尾，现在看到的应该是这样，



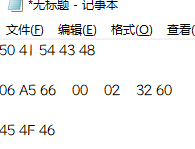
中间的一排字节就是ips所修改的ROM内容，

前面的三个字节代表地址，

00含义未知，

02代表修改的字节长度，可以看到02后面刚好2个字节

这时候就可以把内容分开，



像这样，一目了然，

地址 + 00 + 修改的字节长度 + 修改的字节内容

我在之前的教程有说过，调试器找到的汇编地址想在ROM定位到，

若没有六位要在其第一位加1，反之减1，有点绕，但大概就是这意思，

简单说这里的06A566在调试器内存浏览区域是无法定位到正确地址的，

要在其前加1，也就是16A566

其后的字节内容也是经过了二字节交叉的，若要将其转化为作弊码，需将其再次二字节交叉，

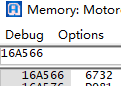
也就是6032

这样就可以推理出 16A566 = 6032

当然还不够，改ROM汇编是要还原的，现在带调试器进入游戏，

在内存浏览区域键入16A566并回车两次，

可以看到16A566的原字节码为6732



将其转化为作弊码也就是

<cheat desc="通用 - 解除武器限制 原版用">

<script state="run">

<action>maincpu.rw@16A566=6032</action>

</script>

<script state="off">

<action>maincpu.rw@16A566=6732</action>

</script>

</cheat>

将其写入作弊文件，重新载入作弊文件，并开启这一项，

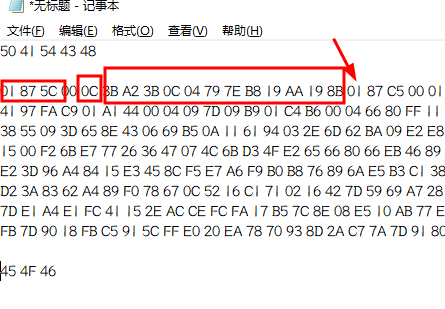


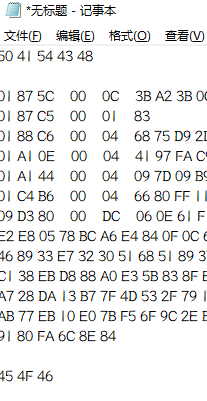
测试没问题，血赵云装备方天画戟释放日月双华

其次是加密的，拿31-119的全攻分析，前面说过的不再赘述，

将其ips内容粘贴到记事本并分开，值得一提的是，像遇到这种很多的字节时不要头痛，

其实是有规律的，前面3个字节依然是地址，00不管，0C为字节长度，转化为10进制也就是12个字节，也就是说8B后面的01就是下一个地址的内容了





将其分开后就是这样，也就是说实际上只有七个地址块，当然实际上不只，

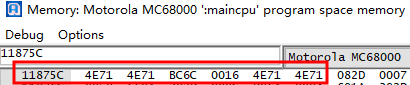
这里我只拿第一个举栗，也就是01875C，未满六位第一位加1，等于11875C，

因为这是用ROM比较差异制作出来的ips，其内容也是附加进ROM之后才解密

简单说这里所修改的的字节没有任何意义，我们需要的只是地址，以及字节长度

先将ips附加进ROM，直接加载还是打入ROM自己决定，

然后在调试器内存浏览区域键入11875C，并回车两次，会看到如图所示



留意之前地址后跟着的修改字节长度是0C也就是12个字节，

68K看字节是从左到右看，也就是这一排被框中的

将其转化：

11875C = 4E71

11875E = 4E71

118760 = BC6C

118762 = 0016

118764 = 4E71

118766 = 4E71

这个地址就算是记录完成，再加载原版ROM，记录还原字节，将其转化为作弊码：

<cheat desc="全屏攻击 Part1">

<script state="run">

<action>maincpu.rw@11875C=4E71</action>

<action>maincpu.rw@11875E=4E71</action>

<action>maincpu.rw@118760=BC6C</action>

<action>maincpu.rw@118762=0016</action>

<action>maincpu.rw@118764=4E71</action>

<action>maincpu.rw@118766=4E71</action>

</script>

<script state="off">

<action>maincpu.rw@11875C=6E00</action>

<action>maincpu.rw@11875E=01B4</action>

<action>maincpu.rw@118760=BC6C</action>

<action>maincpu.rw@118762=0016</action>

<action>maincpu.rw@118764=6D00</action>

<action>maincpu.rw@118766=01AC</action>

</script>

</cheat>